Patent Application No. 09/754,813

REMARKS

This Amendment is in response to the Office Action dated January 31, 2003. In the Office Action, claims 1-20 were rejected under 35 USC §102. Currently pending claims 1-15 and 17-20 are believed allowable, with claims 1, 11, and 18 being independent claims.

CLAIM OBJECTIONS:

Claims 18-20 were objected to for incorrect dependency. After careful inspection of claims 18-20, the applicant respectfully submits that claims 18-20 are in compliance with 35 USC §112 and that dependency correction is not required. If objection to claims 18-20 is maintained, the applicant respectfully requests more detail as to the reason for this objection.

CLAIM REJECTIONS UNDER 35 USC §102:

Claims 1-20 were rejected under 35 USC §102 as being anticipated by U.S. Patent No. 6,134,551 to Aucsmith (herein "Aucsmith"). Aucsmith appears to disclose a technique for determining whether a key, such as a credit number, is a member in a database containing invalid keys. *Aucsmith*, col. 1, lines 15-19. Aucsmith teaches maintaining a local invalidity cache of a remote database stored on a server. *Aucsmith*, col. 2, lines 58-61 and Fig. 2. Rather than storing all the individual invalid keys of the remote database in the local invalidity cache, the local cache contains a hash function of all the invalid keys in the remote database. *Aucsmith*, col. 2, lines 63-65. Thus, if a lookup in the local cache is performed and a particular key is not found in the local cache, then that key is guaranteed not to be a member of the remote database. *Aucsmith*, col. 3, lines 30-33. On the other hand, if a lookup reveals that the key is found in the local cache, further communication between the client and server must be performed to determine if the key is indeed a member of the remote database. *Aucsmith*, col. 3, lines 35-52.

In contrast with Aucsmith, the present application addresses the problems associated with different certificate authorities (CAs) using

- 6 -

different certificate revocation list (CRL) distribution mechanisms to identify revoked digital signature certificates. *Application*, page 4, lines 12-28. Broadly speaking, the invention uses different retrieval agents to consolidate CRLs from different CAs into a central CRL database, which can be replicated to other machines. *Application*, page 5, lines 4-7. The agents retrieve CRLs using various distribution methods, such as LDAP, HTTP and RFC1424. *Application*, page 11, lines 11-14 and page 16, lines 5-13.

Turning now to the claims of the application, claim 1 recites, in part, "a plurality of CRL databases for storing the consolidated CRLs from multiple CRL retrieval agents and/or the replications of CRLs, the CRL databases storing at least one individually identifiable revoked digital certificate." It is respectfully submitted that this limitation is not disclosed or suggested in Aucsmith. Although, as pointed out by the Examiner, Aucsmith recites an Invalidity Database **222** and a Local Invalidity Cache **218**, these elements cannot be characterized as storing consolidated CRLs from multiple CRL retrieval agents and/or the replications of CRLs, and storing at least one individually identifiable revoked digital certificate. According to Aucsmith, the Invalidity Database **222** includes "a list of revoked credit card numbers, ID badge numbers, or other unique values which are no longer valid." *Aucsmith*, col. 3, lines 17-19. Thus, the Invalidity Database **222** cannot be defined as consolidating CRLs from multiple CRL retrieval agents and/or the replications of CRLs. Furthermore, the Invalidity Cache **218** comprises "a bloom filter which is generated by performing one or more hash functions of the invalid keys contained in the invalidity database **222** stored in the server." *Aucsmith*, col. 3, lines 26-30. Thus, the Invalidity Cache **218** is a transform of the Invalidity Database **222** contents. It is therefore respectfully submitted that the Invalidity Cache **218** cannot be characterized as a CRL database of claim 1 of the present application. Moreover, the bloom filter hashes all keys contained within the Invalidity Database **222** and therefore cannot satisfy the requirement of claim 1 that the CRL databases store at least one individually identifiable revoked digital certificate. *Aucsmith*, col. 3, lines 57-63.

- 7 -

In addition, claim 1 recites, in part, "said system enabling consolidation and access of the certificate revocation lists (CRLs) from the plurality of certificate authorities (CAs)." As discussed above, Aucsmith discloses a local cache containing a hash function of all the invalid keys in a remote database. It is respectfully submitted that Aucsmith does not mention or suggest consolidating certificate revocation lists from a plurality of certificate authorities (CAs). For at least the above-stated reasons, claim 1 is believe not anticipated by Aucsmith and is therefore allowable over the cited art.

Claim 2 of the present invention is dependent on claim 1 and recites, in part, a "central CRL database for storing the consolidated CRLs from the multiple CRL retrieval agents." Although Aucsmith is cited as teaching these limitations at Fig. 2 and col. 3, lines 14-67, it is respectfully submitted that Aucsmith does not teach or suggest storing consolidated CRLs from multiple CRL retrieval agents. It is further submitted that these elements are not found in Aucsmith because the patent does not address the issues of different CAs using different CRL distribution mechanisms to identify revoked digital signature certificates. Aucsmith discloses a hash function of all the invalid keys in a remote database as a means of reducing communications between a client and server. *Aucsmith*, col. 3, lines 30-34. Thus, Aucsmith does not teach or suggest the limitations recited in claim 2. For at least is reason and the reasons for allowance of claim 1, claim 2 is believed allowable.

Claim 3 of the present invention is dependent on claim 1 and further recites a LDAP/CRL retrieval agent for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases. In rejecting this claim, Aucsmith is cited at column 3, lines 53-67 as inherently including a LDAP server. After careful review of the cited passage, it is respectfully submitted that the cited text does not teach or suggest a LDAP server. Furthermore, no basis in fact and/or technical reasoning to support the determination that a LDAP server is a <u>necessary</u> inherent characteristic of the cited passage. See MPEP §2112. Thus, it is respectfully submitted that for at least these

- 8 -

reasons and the reasons for allowance of claim 1, claim 3 is believed allowable.

Claim 4 of the present invention is dependent on claim 1 and further recites a HTTP/CRL retrieval agent for periodically retrieving CRLs from specified HTTP servers and updating the CRL database. In rejecting this claim, Aucsmith is cited at column 3, lines 53-67 as inherently including a HTTP server. After careful review of the cited passage, it is respectfully submitted that the cited text does not teach or suggest a HTTP server. Furthermore, no basis in fact and/or technical reasoning to support the determination that a HTTP server is a _necessary_ inherent characteristic of the cited passage. See MPEP §2112. Thus, it is respectfully submitted that for at least these reasons and the reasons for allowance of claim 1, claim 4 is believed allowable.

Claim 5 of the present invention is dependent on claim 1 and further recites RFC1424/CRL retrieval agents for periodically sending RFC1424/CRLs retrieval request and receiving CRL retrieval reply. In rejecting this claim, Aucsmith is cited at column 3, lines 53-67. After careful review of the cited text, it is respectfully submitted that that the text does not teach or suggest RFC1424/CRL retrieval agents for periodically sending RFC1424/CRLs retrieval request and receiving CRL retrieval reply. Thus, it is respectfully submitted that for at least this reason and the reasons for allowance of claim 1, claim 5 is believed allowable.

Claim 6 of the present invention is dependent on claim 1 and further recites a Http receiver agent triggered by a HTTP request, the Http receiver agent verifies an authorization of the requester, if successful, the agent stores each transmitted CRL in the CRL databases. In rejecting this claim, Aucsmith is cited at column 7, lines 12-42. After careful review of the cited passage, it is respectfully submitted that that the cited text does not teach or suggest a Http receiver agent triggered by a HTTP request, the Http receiver agent verifies an authorization of the requester, if successful, the agent stores each transmitted CRL in the CRL databases. Thus, it is respectfully

- 9 -

Patent Application No. 09/754,813

submitted that for at least this reason and the reasons for allowance
of claim 1, claim 6 is believed allowable.

Claim 7 of the present invention is dependent on claim 1 and
additionally recites that the CRL retrieval agents further verify the
integrity and the authenticity of the retrieved CRLs. In rejecting
this claim, Aucsmith is cited at column 3, lines 35-40. It is
respectfully submitted that the cited text does not teach or suggest
CRL retrieval agents verifying the integrity and the authenticity of
retrieved CRLs. Thus, it is respectfully submitted that for at least
this reason and the reasons for allowance of claim 1, claim 7 is
believed allowable.

Claim 8 of the present invention is dependent on claim 1 and
further recites particular replication architecture is used among the
plurality of CRL databases in order to maintain database consistency.
In rejecting this claim, Aucsmith is cited at column 3, lines 63-67.
After careful review of the cited passage, it is respectfully submitted
that the cited text does not teach or suggest particular replication
architecture used among a plurality of CRL databases in order to
maintain database consistency. Thus, it is respectfully submitted that
for at least this reason and the reasons for allowance of claim 1,
claim 8 is believed allowable.

Claim 9 of the present invention is dependent on claim 2 and
further recites a hub-and-spoke replication architecture is used among
the central CRL database and the plurality of CRL replication
databases. In rejecting this claim, Figs. 2 and 5 of Aucsmith are
cited. After careful review of these figures, it is respectfully
submitted that a hub-and-spoke replication architecture used among a
central CRL database and a plurality of CRL replication databases is
not shown or suggested in Aucsmith. Thus, it is respectfully submitted
that for at least this reason and the reasons for allowance of claim 2,
claim 9 is believed allowable.

Claim 10 of the present invention is dependent on claim 1 and
further recites that the system is also adapted for consolidating and
accessing at least one kind of black list. In rejecting this claim,

- 10 -

Aucsmith is cited at column 3, lines 14-22. After careful review of
the cited passage, it is respectfully submitted that that the cited
text does not teach or suggest that a system adapted for consolidating
and accessing at least one kind of black list. Thus, it is
respectfully submitted that for at least this reason and the reasons
for allowance of claim 1, claim 10 is believed allowable.

Claim 11 of the present invention recites, in part, storing
consolidated CRLs from multiple CRL retrieval agents or the
replications of CRLs into a plurality of CRL databases, the
consolidated CRLs including at least one individually identifiable
revoked digital certificate. It is respectfully submitted that this
limitation is not disclosed or suggested in Aucsmith. As discussed
above, the Invalidity Database 222, being "a list of revoked credit
card numbers, ID badge numbers, or other unique values which are no
longer valid," cannot be characterized as consolidated CRLs from
multiple CRL retrieval agents or the replications of CRLs. *Aucsmith,*
col. 3, lines 17-19. Furthermore, the Invalidity Cache 218, being a
transform of the Invalidity Database 222, cannot be characterized as
consolidated CRLs from multiple CRL retrieval agents or the
replications of CRLs into a plurality of CRL databases. Thus, for at
least the above-stated reasons, claim 11 is believe not anticipated by
Aucsmith and therefore allowable over the cited art.

Claim 12 of the present invention is dependent on claim 11 and
recites, in part, a "central CRL database and a plurality of CRL
replication database, said central CRL database for storing the
consolidated CRLs from multiple CRL retrieval agents." Although
Aucsmith is cited as teaching these limitations at Fig. 2 and col. 3,
lines 53-67, it is respectfully submitted that Aucsmith does not teach
or suggest storing consolidated CRLs from multiple CRL retrieval
agents. It is further submitted that these elements are not found in
Aucsmith because the patent does not address the issues of different
CAs using different CRL distribution mechanisms to identify revoked
digital signature certificates. Aucsmith discloses a hash function of
all the invalid keys in a remote database as a means of reducing
communications between a client and server. *Aucsmith,* col. 3, lines

- 11 -

30-34. Thus, for at least these reasons and the reasons for allowance of claim 11, claim 12 is believed allowable.

Claim 13 of the present invention is dependent on claim 11 and further recites consolidating and accessing all kinds of black lists. In rejecting this claim, Aucsmith is cited at column 3, lines 14-22. After careful review of the cited passage, it is respectfully submitted that that the cited text does not teach or suggest consolidating and accessing all kinds of black lists. Thus, it is respectfully submitted that for at least this reason and the reasons for allowance of claim 11, claim 13 is believed allowable.

Claims 14-17 are dependent on and further limit claim 11. Since claim 11 is believed allowable over the cited art, claims 14-17 are also believed allowable.

Claim 18 of the present invention recites, in part, storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases, the consolidated CRLs including at least one individually identifiable revoked digital certificate. It is respectfully submitted that this limitation is not disclosed or suggested in Aucsmith. As discussed above, the Invalidity Database 222, being "a list of revoked credit card numbers, ID badge numbers, or other unique values which are no longer valid," cannot be characterized as consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs. *Aucsmith,* col. 3, lines 17-19. Furthermore, the Invalidity Cache 218, being a transform of the Invalidity Database 222, cannot be characterized as consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases. Thus, for at least the above-stated reasons, claim 11 is believe not anticipated by Aucsmith and therefore allowable over the cited art.

Claims 19-21 are dependent on and further limit claim 18. Since claim 18 is believed allowable over the cited art, claims 19-21 are also believed allowable.

- 12 -

Patent Application No. 09/754,813

CONCLUSION

In view of the forgoing remarks, it is respectfully submitted that this case is now in condition for allowance and such action is respectfully requested. If any points remain at issue which the Examiner feels could best be resolved by a telephone interview, the Examiner is urged to contact the attorney below.

The applicant hereby petitions for a one-month extension of time for response. Please charge Deposit Account 50-0510 a one-month extension fee in the amount of $110 due with this Amendment. No additional fee is believed due with this Amendment, however, should an additional fee be required please charge Deposit Account 50-0510 the required fee. Should any additional extensions of time be required, please consider this a petition thereof and charge Deposit Account 50-0510 the required fee.

Respectfully submitted,

Dated: June 2, 2003

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
69-60 108th Street, Suite 503
Forest Hills, NY 11375
Telephone (718) 544-1110
Facsimile (718) 544-8588

- 13 -